CRYPTOGRAPHIC KEY DISTRIBUTION USING KEY UNFOLDING

Abstract of the Disclosure

Methods, computer-readable media, and apparati for securely distributing a cryptographic key (C) from a first party(s) to a second party(s). A method embodiment of the present invention comprises the steps of combining (steps 1 and 2) the cryptographic key (C) with a fresh transport key (T) to form a key set; unfolding (step 10) a previous transport key (T) to form an unfolded transport key (UT); encrypting (step 7) the key set using the unfolded transport key (UT) to form an encrypted key set; distributing (step 8) the encrypted key set across a medium (3); and decrypting (step 9) the encrypted key set using the unfolded transport key (UT) to reconstitute the cryptographic key (C) and the transport key (T).